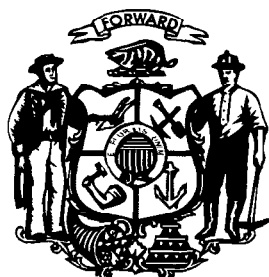


General Records Schedule:

Data Security and Related Records



For use by
State of Wisconsin Government Agencies

July 2001

Public Records Board

RDA # 904001 – 9040110

Table of Contents

Letters of Endorsement

Division of Information Technology Services	iii
LAB, PRB, and DOA Records Officer	v
Purpose	1
Who May Use This Schedule	1
Scope	1
Records Functions Included	1
Interrelated Records Cross-referenced	1
Records <u>Not Included</u>	1
Electronic Records	1
For Effective Use of This Schedule	2
Identify Official, Agency, and Working Copies.....	2
Records Series Title and Categories	2
A Tool to Develop and Maintain Documentation of Data Security Policies, Procedures, Transactions and Control.....	2
Records Related to The Use of Federal Funds.....	3
Retaining Records	3
Delaying Records Destruction	3
Maintaining Inactive Records	3
Confidentiality of Data Security-Related Records	3
Personally Identifiable Information	4
For Additional Information and Assistance	4
Legend Of Terms and Phrases	4
Description of Statewide Agency Security Records	7



**WISCONSIN DEPARTMENT OF
ADMINISTRATION**


SCOTT McCALLUM
GOVERNOR

GEORGE LIGHTBOURN
SECRETARY

Division of Information Technology
101 East Wilson St., 4th Floor
Post Office Box 8974
Madison, WI 53708-8974
Voice (608) 264-9516
Fax (608) 266-5055 TTY (608) 267-9629
Web Site: www.doa.state.wi.us/infotech/

DATE: July 6, 2001

TO: State Agency and Wisconsin Technical College Systems Security Officers

FROM: Sari King, Administrator, Info-Tech Services, 

SUBJECT: General Records Schedule: Data Security and Related Records

The attached statewide General Records Schedule: Data Security and Related Records was approved by the Public Records and Board. This document provides guidance for managing data security-related records to meet all reasonable retention needs. Retention periods specified in the general schedule are sufficient for legal purposes.

State agency data security staff should follow the retention periods established in the schedule and routinely destroy records after the time periods specified have passed. Defer routine records destruction in cases involving litigation, court orders, open records requests, or outstanding audits until these issues are resolved.

If you have questions about the legal interpretation of a security-related record, you should first contact your agency legal staff.

Special thanks to Valerie Clemen and Info-Tech Mainframe Security Officer Carolyn Buller for taking leadership roles in developing this document, and to the state agency data security or records officers who contributed their time and energy.

If you have questions about the interpretation and implementation of this records schedule, contact your agency's designated data security officer or records officer. If you need additional assistance, you may contact Harold Coltharp, (608) 266-2770, or Steve Hirsch, (608) 266-2996, of the DOA Records Management Section.



**WISCONSIN DEPARTMENT OF
ADMINISTRATION**

**STATE OF WISCONSIN
PUBLIC RECORDS BOARD**

**SCOTT McCALLUM
GOVERNOR**

**Steve Hirsch
EXECUTIVE SECRETARY**

DATE: May 11, 2001

TO: State Agency Data Security Officers,
Wisconsin Technical College Systems Security Officers
State Agency Records Officers, and
Employees working with data security records

SUBJECT: General Records Schedule: Data Security and Related Records

The revised statewide General Records Schedule: Data Security and Related Records was approved by the Public Records Board. In most cases, agency staff should follow the retention periods in this schedule and routinely destroy records after the time periods specified have passed. No further approval is needed from either DOA or the Public Records Board. Under special circumstances, the records may need to be saved longer.

State agency data security officers will be working together to bring existing records into conformance with the schedule. A letter endorsing this general schedule from DOA's Information Technology Services Deputy Administrator is also attached.

We want to thank Info-Tech's Computer Systems Security Officer Carolyn Buller for her continued support and contributions to the creation of this document. Thanks also to those security officers and records managers that participated in the document's development.

If you have any questions about the interpretation and implementation of this records schedule, please contact your agency security officer or records officer. For additional assistance, you may contact Steve Hirsch or Harold Coltharp at DOA's Records Management and Transportation Section, (608) 266-2996 or (608) 266-2770.

Bryan Naab
Financial Audit Director
Legislative Audit Bureau

Steve Hirsch
PRB Exec. Secretary

cc: Carolyn Buller
Harold Coltharp

General Record Schedules

PURPOSE

The purpose of this schedule is to:

- Provide agencies with uniform guidelines for the retention and disposition of common data security and related records;
- Ensure that agencies retain data security records as long as needed for internal administration, and to meet legal, fiscal, and other state of Wisconsin and federal requirements;
- Promote cost-effective management of records;
- Comply with the state of Wisconsin legal requirements and the Legislative Audit Bureau's audit requirements; and
- Provide agencies with legal authorization to dispose of obsolete records on a regularly scheduled basis after minimum retention periods.

WHO MAY USE THIS SCHEDULE?

Agencies Included: Except for the University of Wisconsin System, this general schedule applies to all Wisconsin state agencies, and the Wisconsin Technical College System.

All agencies will find the records series categories and retention periods listed in this document relevant in managing data security and related records. Agencies not covered by this schedule are encouraged to adopt retention schedules for their computer-related data records.

SCHEDULE DOES NOT REQUIRE CREATION OF RECORDS

It is understood that every agency may not have every type of record listed in this schedule. This schedule does not require records to be created by state agencies. It provides policy guidance for those records that are used by any agency.

SCOPE

This general schedule covers records series that agencies create and use for data security functions. To make the document as usable as possible, the information is presented by functional areas. Agencies may use different terminology and may file records series differently.

However, the functional areas should be similar for all agencies and the retention periods apply, regardless of the filing arrangement used. **If records series with varying retention periods are filed together as a unit, the retention period of the longest record series will control all the record series in the file.**

This schedule applies to data security and related records regardless of who maintains them. For instance, the schedule applies to state-wide processing centers, such as the DOA Division of Information Technology Services, central agency IT operations, and those administered by agency program areas.

Electronic Records: For electronic or machine-readable security data systems, this schedule applies to the electronic security information maintained by state agencies. Agency security officers may receive copies of the information and/or generate their own electronic related records.

If agencies have additional data security-related records that are not covered, contact the resources listed in the section "For Additional Information and Assistance," prior to developing a separate general schedule.

FOR EFFECTIVE USE OF THIS SCHEDULE

Identify the Official Record and the Agency Record Copy: Some data security records are produced, in multiple. This schedule covers all copies of the record, including the following:

Official Record: The official record is the information that is most likely to be used for multi-agency audit purposes, regardless of the information's medium. The official record must be identified by each state agency for all records series. **The official record holder is the agency that performs the task.**

Agency Copy: The agency should also identify the agency copy and its location in the agency. The agency copy is the copy that must be retained to satisfy any agency-specific audit or legal requirement of the agency's operation. The agency copy is held by the agency that made the request.

Working Copies: All other copies of the record are considered working or convenience copies. In the interest of efficiency, *do not keep these copies longer than needed*. If you do not need convenience copies in the office, discard them as soon as practical. **Do not send them to the State Records Center.**

Note: Generally, working copies should not be retained longer than the official record and agency copies of the record, because of the costs associated with maintaining them. If an agency continues to retain convenience copies beyond the retention periods set for official and agency copies, the agency will need to provide appropriate access to these copies in response to audit or legal requests and per open records laws

Records Series Titles and Categories: Titles of records series may not be the exact titles used by an agency for each record or records series. The schedule requires some interpretation and application to specific agency titles of data security records. If agency staff are uncertain about the schedule's application to a specific group of records or need assistance, see "For Additional Information and Assistance" section to identify sources for advice.

THE SCHEDULE IS A TOOL TO DEVELOP AND MAINTAIN DOCUMENTATION OF DATA SECURITY POLICIES, PROCEDURES, TRANSACTIONS, AND CONTROL

Agencies need to maintain adequate documentation of data security transactions and activities to meet internal administrative needs, legal mandates, and program and financial audit requirements. This schedule provides agency staff with a sound basis for adequate program documentation.

Agency records management officers should work with agency data security officers to implement organized filing systems and to design information processes that are consistent with effective, efficient records management principles, and design filing systems to meet staff informational needs and facilitate cross-reference to retention and disposition guidance in this schedule.

Each agency should use this schedule to continuously dispose of records that are no longer needed. Each agency should implement these retention and disposition policies in a timely and efficient manner. To facilitate disposition, agency staff should cut off files periodically and develop methods to mark files when they close.

The disposition for all the series is "destroy confidential", since they don't contain historically significant material.

RECORDS RELATED TO THE USE OF FEDERAL FUNDS

Agencies may receive funds from state and federal sources. This general schedule covers all records, regardless of funding source. Retention schedules developed in this schedule meet or exceed federal retention requirements, as contained in the "Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments (Common Rules)."

If a federal agency requires retention of records for longer periods than those provided in this schedule, agency staff should obtain specific, written directions from the federal agency, detailing retention requirements and indicating terms and conditions to be followed. In addition, agency staff should contact officials in the identified areas of data security and the Public Records Board, so that the situation can be investigated.

RETAINING RECORDS

Agencies are required to follow this schedule for applicable records. Retention periods established and disposition directions are state policy requirements for data security records. Records may be delayed from destruction only under the following conditions:

- Particular records have been identified as needed for a financial or performance audit;
- Records are needed for an actual or imminent legal proceeding;
- An open records request for particular records has been received and not completed; or
- Retention schedules are under revision.

The Wisconsin Open Records Law, s. 19.35(5), Wis. Stats., *forbids the destruction of any record after an inspection or copying request until the request is granted, or at least 60 days after the date that the request is denied.* Court orders may extend this time period. The agency's legal custodian of records can provide advice.

It is the responsibility of the office holding the record to determine if an audit, litigation, an open records request, or retention schedule revision is pending before disposing of that record.

Official records and agency copies of inactive records that must be retained for an additional period of time before the expiration of their legal retention requirements, should be transferred to a low-cost, inactive records facility, such as the State Records Center.

CONFIDENTIALITY OF DATA SECURITY-RELATED RECORDS

Some security records may be confidential. In general, the records in this schedule are likely to be open if they relate to program operations and administration and do not contain information on individuals. Those records that relate to individuals are more likely to contain confidential information. If in doubt as to whether or not a specific record is confidential, it is always a good idea to check with the agency legal counsel or records officer. If your agency does not have a legal counsel, an assistant attorney general in the Department of Justice should be able to provide advice.

The terms "destroy" is used throughout the document for those records without secondary historical value. Destroy, in a confidential manner, all security-related records that contain information on individuals. Contact the Department of Administration (DOA) Records Management Section (608-266-2996) to discuss options for confidential destruction of records. Outlying areas should use locally available facilities capable of meeting state criteria for confidential disposal of records.

PERSONALLY IDENTIFIABLE INFORMATION

Some data security computer-related records in this schedule contain personally identifiable information within the meaning of this term, as defined in s. 19.62(5), Wis. Stats. Agencies should be aware of the requirements in Subchapter IV, Personal Information Practices, of Chapter 19 of the state statutes. These requirements were not eliminated when the state Privacy Council and Privacy Advocate were eliminated.

FOR ADDITIONAL INFORMATION AND ASSISTANCE

Agency security officers and program staff should also consult with the following resource staff for additional information and assistance with records management concerns.

DOA Records Management Section: The DOA Records Management Section provides free training sessions, as needed, on implementation of general records schedules.

Agency Records Officer: Each agency has a designated records officer who serves as liaison to the Public Records Board. The records officer is responsible for agency-wide records management (RM) planning, program development, and miscellaneous RM assistance, to name a few areas.

Public Records Board: The board's Executive Secretary can offer technical assistance and training to assist agencies with records management, including records scheduling and interpretation of schedules.

State Historical Society: The State Historical Society of Wisconsin (SHSW) assists agencies in managing records, particularly in identifying the small percentage of records that have historical value.

LEGEND OF TERMS AND PHRASES

For each record series identified below, the schedule provides the records series identifying number, title, additional description and sometimes a comment on the administration of this series. Also included is the location/custodian, which indicates where the record is likely to be maintained. And last, the retention and disposition are specified.

Retention is the period of time that the records must be retained to satisfy all state requirements. These are the types of retentions:

- *Creation* plus a period of time: CR is the designation for these types of retentions.
- *Event* plus a period of time: EVT is the designation for these types of retentions. Event type retentions require a specified event to start the "clock ticking" on the retention period. The event should be well defined, as part of the record series, and understood by all staff who work with the records.
- *FIS* stands for current FIScal year

Disposition is what happens to the records after the retention period is satisfied. Most record series in the schedule have a disposition of "Destroy". The State Records Center has fact sheets that explain options for destruction of paper and microfilm records.

LAB Mandate: Under sec. 13.94, Wis. Stats., the Legislative Audit Bureau (LAB) is mandated to audit agencies every three (3) years.

Legal Requirements/Statute of Limitation for Computer Crimes: Under sec. 939.74, Wis. Stats., the statute of limitation is 6 years for a felony and 3 years for a misdemeanor.

Description of Statewide Agency Security Records

90400010 Requests for Users Access

Records may include, but are not limited to, requests for changes to access and Dial-Up.

Location: Official/implementor file
Retention: Official: Retain FIS +3
 Agency/requestor file: Same as official file.
 Working: Retain until no longer needed.
Disposition: Destroy confidential
Justification: Meets audit requirements and administrative needs of the agency

90400020 Confidentiality Form

Records include employee acknowledgement of security-related responsibilities, such as data confidentiality form or employee password security agreements.

Location: Official file: Hiring Agency.
Retention: Event EVT +8 years (event = departure of employee)
Disposition: Destroy confidential
Justification: Exceeds LAB and exceeds federal requirements and complies with Computer Crime Law, s. 939.74, Wis stats.

90400030 Logon ID Request Acknowledged by User

Records that include an acknowledgement of the user responsibilities, date of such acknowledgement and the logon id requested.

Location: Official file: Implementing agency or Info-Tech Services (only Info-Tech and small agencies w/o security officer).
Retention: Official/implementor file: EVT +8 years (event = departure of employee)
 Agency/requestor file: Same as official file.
 Working: Retain until no longer needed.
Disposition: Destroy confidential
Justification: Exceeds LAB and federal requirements and complies with Computer Crime Law, s. 939.74, Wis stats.

90400040 Logon ID Authorized by Supervisor

Records that do include a dated and authorized logon id request, but do not include acknowledgment of user responsibility.

Location: Official file: Implementing agency or Info-Tech Services (only Info-Tech and small agencies w/o security officer).
Retention: Official/implementor file: FIS+3 years
Agency/requestor file: Same as official file.
Working: Retain until no longer needed.
Disposition: Destroy confidential
Justification: Meets audit requirements and administrative needs of the agency

90400050 Public Logon ID Request

Records that include an acknowledgement of the user responsibilities, date of such acknowledgement and may include the public logon id requested.

Location: Official file: Implementing agency or Info-Tech Services (only Info-Tech and small agencies w/o security officer).
Retention: Official/implementor file: EVT +8 years (event = removal of logon id)
Agency/requestor file: Same as official file.
Working: Retain until no longer needed.
Disposition: Destroy confidential
Justification: Exceeds LAB and federal requirements and complies with Computer Crime Law, s. 939.74, Wis stats.

90400060 Enterprise Security Committee Minutes—Electronic Minutes from biweekly meeting of agency security officers.

Records include minutes from biweekly meetings where policy may be set or revised; and security privileges may be granted or revoked.

Location: Official file: Info-Tech Services.
Retention: FIS +3 years
Disposition: Destroy confidential
Justification: Meets audit requirements and administrative needs of the agency

90400061 Agency Security Committee Minutes

Records include agency security committee minutes regarding discussions about security planning activities, development of security policies, identification of security exposures, and remedial measures.

Location: Official file: Agency conducting security meeting
Retention: Retain until no longer needed
Disposition: Destroy confidential
Justification: Minutes documenting agency discussions regarding security are public record, unless classified as confidential by statute. The retention length of such records is determined by each agency, based solely on its administrative value to the agency. There is no legal or audit retention requirement.

90400070 Security Handbook—Paper

Records may include security action (procedures) reference guide.

Location: Official file: Info-Tech Services
Retention: EVT (event = record is superseded)
Disposition: Destroy confidential
Justification: There is no legal or audit requirements to retain such records.

90400080 Assignment and Authorization of Security Officer

Records may include: Request from agency head or delegated authority and forwarded to the requesting agency's or Info-Tech's security officer.

Location: Official file: Implementing agency
Retention: Implementing agency retain until EVT (event = departure of security officer).
Agency: Until no longer needed
Disposition: Destroy confidential
Justification: LAB audits forms for current security officer/representative authorizations.

90400090 Security Reports

Records may include the following reports and can be in electronic or paper format: daily events, restricted LID log, info-storage violations, info-storage log, data set traces, logging and violations, daily by-pass label processing, resource tracing and violation for all platforms and applications.

Location: Official file: Info-Tech Services or agency owning the data or logs.
Retention: FIS +3
Disposition: Destroy confidential

Justification Meets audit requirements and administrative needs of the agency

90400100 Security-Related Network Usage Logs

Logs contain information about the use of network services. Agencies determine which logs contain high-risk records, such as those providing security information about system usage. Maintain logs that track communications considered to be a risk to the agency based on agency operations and the applications affected. The logs may include network operating system logs (such as NT security logging etc.) or other network monitoring (such as intrusion detection devices, modem pool logs, central web cache logs, network flows generated by routers, firewall logs, DHCP logs, e-mail server logs, web servers logs, NT security logs, UNIX system logs, etc).

Location: Official file: Agency owning data.
Retention: CR +1 yr. Extended time period if the records are needed to meet other issues, e.g. billing, statistics, etc.
Disposition: Destroy confidential
Justification: Logs can contain sensitive information about security events on the network and should be retained for legal, audit, and administrative purposes.

90400110 Low-Risk Usage Logs

These logs contain low risk, but high volume information about network usage. Agencies determine the risk and potential use of network logs. If the logs track communications that are considered low risk, based on their operations and applications affected, the retention value is low. For instance, depending on agency, central web caching or network flow generated by routers may be large and considered lower risk. The logs may include network operating system logs or other network monitoring (such as intrusion detection devices, modem pool logs, central web cache logs, network flows generated by routers, firewall logs, DHCP logs, e-mail server logs, web servers logs, NT security logs, UNIX system logs, etc).

Location: Official file: Agency that owns data.
Retention: CR +2 weeks -1 yr. (At the discretion of the owner based on need, two week minimum, but 1 year is recommended). The retention periods should be extended if needed to meet other needs, e.g. billing, statistics, legal etc.
Disposition: Destroy confidential
Justification: Logs can contain sensitive information about security events on the network and should be retained for legal and administrative purposes.